UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISON

DODIE WADEN, individually, and on behalf of all others similarly situated, Plaintiff, v. AVEN FINANCIAL, INC, Defendant.	**CASE NO.:** 3:24-cv-00266-MGL **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Dodie Waden ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Aven Financial, Inc. ("Aven" or "Defendant"), and makes the following allegations based upon information, attorney investigation and belief, and upon Plaintiff's own knowledge.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit due to Defendant's failure to properly secure and safeguard sensitive and confidential personally identifiable information ("PII")[1], including the names, Social Security numbers, driver's license numbers and addresses of individuals that had provided information to Defendant for business purposes. Defendant's wrongful disclosure has harmed Plaintiff and the Class (defined below).

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal oridentifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Defendant knew or should have known that due the increasing number of well- publicized data breaches that have occurred in the United States, large data storage such as this require the highest level of protection, which Defendant failed to provide.

3. Plaintiff and members of the Class ("Class Members") entrusted Aven with their sensitive and valuable Personal Information for business purposes. Plaintiff and Class Members did not know that Defendant's data security was inadequate. They did not expect that services offered by Defendant would directly cause such serious injuries that would last for years after the service.

4. Plaintiff brings this action on behalf of all persons in the United States and the South Carolina Sub Class, whose Personal Information was compromised as a result of Defendant's failure to:

i. adequately protect its customers' Personal Information;

ii. warn customers of its inadequate information security practices; and

iii. effectively secure hardware, data, and information systems through reasonable and effective security procedures.

5. Aven's conduct constitutes negligence that proximately caused damages to Plaintiff and Class Members.

6. Plaintiff and Class Members have suffered injury as a direct and proximate result of Aven's conduct.

7. These above-mentioned injuries to Plaintiff and the Class Members include:

a. lost or diminished value of Personal Information, a form of property that Aven obtained from Plaintiff and Class Members;

b. out-of- pocket expenses associated with preventing, detecting, and remediating identity theft and other unauthorized use of their Personal Information;

c. opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to lost time;

d. the continued and certain increased risk that unauthorized persons will access and abuse Plaintiff's and Class Members' unencrypted Personal Information that is available on the dark web; the continued and certain increased risk that the Personal Information that remains in Aven's possession is subject to further unauthorized disclosure for so long as Aven fails to undertake appropriate and adequate measures to protect the Personal Information;

e. invasion of privacy; and

f. theft of their Personal Information and the resulting loss of privacy rights in that information.

8. As a direct and proximate result of Aven's breach of confidence and failure to protect the Personal Information, Plaintiff and Class Members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuses of their Personal Information; ongoing monetary loss and economic harm; loss of value of privacy and confidentiality of the stolen Personal Information; illegal sales of the compromised Personal Information; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries. Plaintiff and Class

Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

9. This Court possesses subject-matter jurisdiction to adjudicate the claims set forth herein under the provisions of the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the Class, including Plaintiff, who are citizens of States diverse from Defendant, and (4) there are more than 100 Class Members.

10. This Court has Personal Jurisdiction over Defendant because Defendant has sufficient minimal contacts with this District. Defendant has purposefully availed themselves to this Jurisdiction through its marketing, sale, advertising, and promotion of its services throughout this Jurisdiction.

11. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391 because Defendant transacts its business in this District, and a substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this District.

PARTIES

PLAINTIFF

12. Plaintiff Dodie Waden is a resident of Richland County, South Carolina.

13. Prior to the data breach, Plaintiff Waden had been a customer of Defendant Aven Financial, Inc.

14. Plaintiff Waden provided Defendant with all PII that was requested required in order to use Defendant's services.

15. Plaintiff Waden received a notice from Defendant dated July 28, 2023 that stated Plaintiff's PII that was collected and maintained by Defendant may have been compromised.

16. Plaintiff Waden has been careful to protect her PII from unnecessary exposure, and only provides her data when it was required.

17. Now that her PII has been exposed in Defendant's breach, Plaintiff Waden will continue to be at a higher risk of cyber-attacks, scam attempts, and identity theft for the foreseeable future.

18. This higher risk will require Plaintiff Waden to invest additional time, energy, money, and stress in order to more closely monitor access to her identity and credit to ensure there is no unauthorized access or attempted fraud.

DEFENDANT

19. Defendant Aven Financial, Inc. is a financial entity headquartered in California, with its principal place of business located at 330 Primrose Rd Ste 412 Burlingame, CA, 94010-4042.

20. Defendant Aven provides low-cost and convenient home equity loans, but useable in the form of a credit card.[2] It works like any other credit card where you can make everyday purchases and earn cash back.[3]

21. Defendant Aven currently operates in 31 states, including South Carolina.[4]

FACTUAL ALLEGATIONS

22. According to its notice letters, on July 17, 2023 a security researcher informed Defendant Aven that he was able to access Aven's internal storage system which contained the personal information of customers.

[2] https://www.aven.com/ (last accessed Jan 17, 2024)
[3] *Id.*
[4] https://www.nerdwallet.com/article/credit-cards/aven-credit-card (last accessed Jan. 17, 2024)

23. After learning that sensitive data was accessible to unauthorized parties, Aven reviewed the compromised files and determined that consumer information had been accessed and leaked.

24. On July 31, 2023, Defendant Aven Financial, Inc. filed a notice of data breach with the Attorney General of Texas after discovering that an unauthorized party was able to access certain information that had been provided to the company.

25. In its notice, Aven stated that the incident resulted in an unauthorized party being able to access consumers' sensitive information, which includes their names, Social Security numbers, driver's license numbers and addresses.

26. Upon completing its investigation, Aven began sending out data breach notification letters to individuals whose information was affected by the recent data security incident.

27. Companies have a legal responsibility to keep the PII that they collect and maintain, secure.

28. By failing to properly manage its vulnerability, Aven has inadvertently allowed access to very sensitive PII of many of its customers.

29. Upon information and belief, the Personal Information stolen in the data breach included customer names, Social Security numbers, driver's license numbers and addresses.

30. Because Aven has exclusive knowledge of what information was compromised for each individual Class Member, Plaintiff reserves the right to supplement her allegations with additional facts and injuries as they are discovered.

31. Plaintiff has suffered actual injury and one or more concrete (real and not abstract), imminent and particularized injuries described below as a direct and proximate result of Aven's deficient data security and failure to protect Plaintiff's Personal Information, as well as Aven's concealment of the same, that allowed unauthorized access to Plaintiff's Personal Information.

32. Had Plaintiff and the Class known that providing Personal Information to Aven would result in their Personal Information being compromised and exfiltrated, Plaintiff and the Class would not have sought Aven's services, would have paid less for them, or would not have provided some or all of their Personal Information to Aven. Thus, Plaintiff and the Class significantly overpaid based on what the services were represented to be compared to what Plaintiff and the Class actually received.

33. In addition to actual, present, concrete, and current injuries, because of Aven's actions and omissions, each and every Plaintiff has suffered, and will continue to suffer perpetual emotional distress, worry, other emotional or psychological harm, and well- founded fear that additional, realistic, objectively-reasonable, threatened, impending, sufficiently imminent harm in the form of identity theft or fraud will occur in the future

34. Had Aven disclosed that it disregarded its duty to protect Plaintiff's Personal Information, or otherwise had insufficient security measures to safeguard and protect Plaintiff's Personal Information from unauthorized access, Plaintiff would have taken this into account in making her decisions.

35. The data breach was the product of a criminal act to gain access to the data. It was the result of a sophisticated, intentional, and malicious attack by professional cybercriminal hackers and was not the result of an accidental disclosure by an Aven employee. Thus, the risk that the victims will experience identity theft or fraud is much more real.

36. Malicious actors often wait months or years to use the Personal Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Personal Information, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

Moreover, although elements of some of Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact that the data breach centralizes the Personal Information and identifies the victims increases the risk to Plaintiff and the Class.

CLASS ACTION ALLEGATIONS

37. Plaintiff bring this action on behalf of themselves, and all others similarly situated pursuant to Rule 23(a) and Rule 23(b)(3) of the Federal Rules of Civil Procedure. Plaintiff seeks class certification on behalf of the classes defined as follows (collectively, "the Class").

Nationwide Class: All persons in the United States who were customers of Aven Financial Inc. and have received notice from Aven Financial Inc. that their data may have been compromised.

South Carolina Sub Class: All persons in South Carolina who were customers of Aven Financial Inc. and have received notice from Aven Financial Inc. that their data may have been compromised.

38. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the court determines whether certification is appropriate.

39. Excluded from the Class are any parent companies, subsidiaries, and/or affiliates, officers, directors, legal representatives, employees, or co-conspirators of Defendant, and all governmental entities, including any judge, justice or judicial officer presiding over this matter.

40. The Nationwide Class and South Carolina Sub Class shall be referred to as the "Class." Proposed Members of said Class will be referred to as "Class Members," or otherwise referenced as "members of the Class."

41. **Numerosity:** The members of the Class are so numerous that joinder of all members of the Class is impracticable. The precise number of Class Members is currently unknown to Plaintiff.

42. **Typicality:** Plaintiff's claims are typical to those of all Class Members because members of the Class are similarly injured through Defendant's uniform misconduct described above and

were subject to their personal data released due to Defendant's conduct. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all members of the Class.

43. **Commonality:** Plaintiff's claims raise questions of law and fact common to all members of the Class, and they predominate over any questions affecting only individual Class Members. The claims of Plaintiff and all prospective Class Members involve the same alleged data breach. These common legal and factual questions include the following:

a. Whether Defendant's data breach exposed their personal information

b. Whether Defendant owed a duty of care to Plaintiff and the Class;

c. Whether Defendant knew or should have known that its data security was inadequate;

d. Whether Defendant wrongfully represent, and continue to represent, that its security is adequate;

e. Whether the alleged conduct constitutes violations of the laws asserted;

f. Whether Defendant's alleged conduct violates public policy;

g. Whether Defendant's representations in advertising are false, deceptive, and misleading;

h. Whether a reasonable consumer would consider the risk of their data being exposed when choosing to do business with Defendant;

i. Whether certification of any or all of the classes proposed herein is appropriate under Fed. R. Civ. P. 23; and

j. Whether Plaintiff and the Class Members are entitled to damages and/or restitution and the proper measure of that loss.

44. **Adequacy:** Plaintiff and her counsel will fairly and adequately protect and represent the interests of members of the Class. Plaintiff has retained counsel experienced in complex litigation and class actions. Plaintiff's counsel has successfully litigated other class action cases like that here, and has the resources and abilities to fully litigate and protect the interests of the Class. Plaintiff intends to prosecute this claim vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class, nor is Plaintiff subject to any unique defenses.

45. **Superiority:** A class action is superior to the other available methods for a fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by Plaintiff and the individual Class Members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for Plaintiff and Class Members, on an individual basis, to obtain meaningful and effective redress for the wrongs done to them. Further, it is desirable to concentrate the litigation of the Class Members' claims in one forum, as it will conserve party and judicial resources and facilitate the consistency of adjudications. Plaintiff knows of no difficulty that would be encountered in the management of this case that would preclude its maintenance as a class action.

46. The Class also may be certified because Defendant has acted or refused to act on grounds applicable to the Class, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

47. Plaintiff seeks preliminary and permanent injunctive and equitable relief on behalf of the entire Class, on grounds generally applicable to the entire Class, to enjoin and prevent Defendant from continuing to provide inadequate data security. Further, Plaintiff seeks for Defendant to provide a full refund of all protective and defensive procedures that Plaintiff and the Class Members have had to employ.

48. Unless a Class is certified, Plaintiff and the Class Members will continue to be injured due to Defendant's conduct. Unless a Class-wide injunction is issued, Defendant may continue to commit the violations alleged and the members of the Class and future customers may continue to be placed in harms' way.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

49. Plaintiff incorporates Paragraph 1-48 by reference as if fully set forth herein.

50. As part of the regular course of its business operations, Defendant gathered and stored the PII of Plaintiff and Class Members. Plaintiff and the Class were entirely dependent on Defendant to use reasonable measures to safeguard their PII and were vulnerable to the foreseeable harm of a security breach should Defendant fail to safeguard their PII.

51. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it— to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

52. Defendant owed a duty of care to Plaintiff and the Class to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

53. Defendant's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including,

as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII by companies such as Defendant's. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

54. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

55. The harm that occurred because of the data breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

56. Defendant gathered and stored the PII of Plaintiff and the Class as part of its business of soliciting its services to its customers which solicitations and services affect commerce.

57. Defendant violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiff and the Class Members, and by not complying with applicable industry standards.

58. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard its customer's PII, and by failing to provide prompt notice without reasonable delay.

59. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to FTCA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and the Class and to minimize the data breach.

60. Defendant's multiple failures to comply with applicable laws and regulations, and the violation of Section of 5 of the FTC Act constitutes negligence *per se*.

61. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

62. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiff could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

63. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class had no ability to protect their PII that was in Defendant's possession.

64. Defendant was in a special relationship with Plaintiff and the Class with respect to the hacked PII because the aim of Defendant's data security measures was to benefit Plaintiff by ensuring that her PII would remain protected and secure. Defendant was the only party able to ensure that its systems were sufficiently secure to protect Plaintiff's and other Class Members' PII. The harm to Plaintiff and the Class from its exposure was highly foreseeable to Defendant.

65. Defendant owed Plaintiff and other Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their PII, including acting to reasonably safeguard such data and providing notification to Plaintiff and the Class of any breach in a timely manner so that appropriate action could be taken to minimize losses.

66. Defendant had duties to protect and safeguard the PII of Plaintiff and the other Class Members from being vulnerable to compromise by taking common-sense precautions

when dealing with highly sensitive PII. Additional duties that Defendant owed Plaintiff and the Class members include:

a. Exercising reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures, and practices to ensure that individuals PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and the Class's PII in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiff and the Class members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

67. Only Defendant was able to ensure that its systems and protocols were sufficient to protect the PII that had been entrusted to them.

68. Defendant breached its duty of care by failing to adequately protect Plaintiff's and the Class's PII. Defendant breached its duty by:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

d. Failing to adequately train its employees to not store unencrypted PII in its personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PII;

f. Failing to mitigate the harm caused to Plaintiff and the Class;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiff and other Class Members of the data breach that affected their PII.

69. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

70. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

71. Defendant's failure to provide timely and clear notification of the data breach to Plaintiff and the Class prevented Plaintiff and the Class from taking meaningful, proactive steps to securing their PII and mitigating damages.

72. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

73. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual

identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to monitor bank accounts and credit reports, prevent, detect, contest, and repair the impact of the PII compromised as a result of the data breach for the remainder of the lives of Plaintiff and the members of the Class.

74. As a direct and proximate result of Defendant's negligence, Plaintiff and the members of the Class have suffered (and will continue to suffer) other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

75. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

76. Plaintiff and members of the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

77. Plaintiff and members the Class seek actual damages, attorney's fees, costs, and any other just and proper relief available thereunder for Defendant's negligent handling of their PII.

COUNT II

NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

78. Plaintiff incorporates Paragraph 1-48 by reference as if fully set forth herein.

79. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Aven of failing to use reasonable measures to protect Personal Information.

80. The FTC publications and orders also form the basis of Aven's duty.

81. Aven violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. Aven's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as Aven, including, specifically the damages that would result to Plaintiff and Class Members.

82. In addition, under state data security statutes, Aven had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Personal Information.

83. Aven's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

84. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

85. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

86. Aven breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information.

87. Plaintiff and Class Members were foreseeable victims of Aven's violations of the FTC Act, and state data security statutes. Aven knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' Personal Information would cause damage to Plaintiff and Class Members.

88. But for Aven's violation of the applicable laws and regulations, Plaintiff's and Class Members' Personal Information would not have been accessed by unauthorized parties.

89. As a direct and proximate result of Aven's negligence per se, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the data breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by Aven; the amount of the actuarial

present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Aven's data breach; lost benefit of their bargains and overcharges for services; nominal and general damages; and other economic and non- economic harm.

COUNT III

BREACH OF CONTRACT
(On Behalf of Plaintiff and the Class)

90. Plaintiff incorporates Paragraph 1-48 by reference as if fully set forth herein.

91. As part of doing business with Defendant, Plaintiff and members of the Class are required to provide Defendant with personal information when entering a contract with Defendant before they are able to receive the benefit of any services from Defendant.

92. Plaintiff and Class Members were customers of Defendant Aven, and therefore had entered a contract with Defendant Aven.

93. Part of that contract, whether expressed or implied, is that Defendant Aven would provide adequate protection of customer's account and personal information, and prevent that data from being given away, sold, or stolen.

94. By failing to adequately update its protection software, Defendant has breached its contract with each Plaintiff and Class Member by proving inadequate protection.

95. This breach has resulted in damages and injuries to Plaintiff and the Class Members, who have had their personal information and account details stolen and thus are more likely to be subject to cyber-attacks, identity fraud, as well as unwanted spam and scam messages.

96. Throughout most of Defendant's history they have provided reasonably proactive data security, preventing many of the cyber-attacks that they have been the target of.

97. Defendant's failure to keep the Plaintiff's and the Class Members' data secure constitutes a material breach of the agreements between Defendant Aven, and Plaintiff and the Class Members. By doing so, Defendant has harmed Plaintiff and each Class Member.

98. Plaintiff and the Class seek actual damages, attorney's fees, costs, and any other just and proper relief available thereunder for Defendant's breach of contract.

COUNT IV

UNJUST ENRICHMENT
(On Behalf of the Plaintiff and the Class)

99. Plaintiff incorporates Paragraph 1-48 by reference as if fully set forth herein

100. This Count is pleaded in the alternative to Count II above.

101. Plaintiff and the members of the Class have conferred a benefit to Defendant in the form of monies paid in interest for convenient home equity loans, among other charges for other services offered by Defendant.

102. Included in these services provided, whether expressed or implied, is the secured protection and safekeeping of Plaintiff's and Class Members' personal and account information.

103. These monies were not given as a gift, but rather with the expectation and understanding that services would be provided in return.

104. Defendant has accepted and appreciated the monies paid, as they have continued to provide its services to Plaintiff and the Class Members, per the terms of their agreements.

105. Then, in July 2023, it was discovered that Defendant had failed and was no longer able to provide safe and secure protection of Plaintiff's and Class Members' data.

106. Defendant has retained all monies paid by Plaintiff and Class Members, even though they have failed to provide the secure service that Plaintiff and Class Members, whether expressed or implied, paid for.

107. Defendant's retention of these monies paid would be inequitable, as Plaintiff and Class Members have paid value for a benefit that they were not provided.

108. Not only was Plaintiff and the Class Members not provided a service for which they paid for, but they will now have to pay additional costs out of pocket in attempts of preventing their data from causing them further harm.

109. Plaintiff and the Class seek actual damages, attorney's fees, costs, and any other just and proper relief available under the laws.

COUNT V

BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

110. Plaintiff incorporates Paragraph 1-48 by reference as if fully set forth herein.

111. This Count is pleaded in the alternative to Count II and Count III above.

112. Aven provides financial services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Aven regarding the provision of those services through their collective conduct.

113. Through Aven's provision of services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Personal Information and PII in accordance with Aven's policies, practices, and applicable law, including the FTC Act.

114. As part of receiving services, Plaintiff and Class Members turned over valuable Personal Information and PII to Aven Accordingly, Plaintiff and Class Members bargained with Defendant to securely maintain and store their Personal Information.

115. Aven violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information.

116. Plaintiff and Class Members have been damaged by Aven's conduct, including by incurring the harms and injuries arising from the data breach now and in the future.

COUNT VI

BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

117. Plaintiff incorporates Paragraph 1-48 by reference as if fully set forth herein.

118. As a condition of obtaining services from Aven, Plaintiff and Class Members gave Aven their Personal Information and PII in confidence, believing that Aven would protect that information. Plaintiff and Class Members would not have provided Aven with this information had they known their information would not be adequately protected. Aven's acceptance and storage of Plaintiff's and Class Members' Personal Information and PII created a fiduciary relationship between Aven and Plaintiff and Class Members. In light of this relationship, Aven must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class Members' Personal Information and PII. Aven has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship.

119. Aven breached that duty by failing to properly protect the integrity of the systems containing Plaintiff's and Class Members' Personal Information and PII, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class Members' Personal Information and PII that it collected, retained, and stored.

120. As a direct and proximate result of Aven's negligence, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the

value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the data breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by Aven; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Aven's data breach; and lost benefit of their bargains and overcharges for services.

COUNT VII

DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

121. Plaintiff incorporates Paragraph 1-48 by reference as if fully set forth herein.

122. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

123. An actual controversy has arisen in the wake of the Aven Financial, Inc. data breach regarding its present and prospective common law and other duties to reasonably safeguard its patients' Personal Information and whether Aven is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Personal Information. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises

of their Personal Information will occur in the future given the publicity around the data breach and the nature and quantity of the Personal Information stored by Aven.

124. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Aven continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. Aven continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

125. The Court also should issue corresponding prospective injunctive relief requiring Aven to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

126. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Aven. The risk of another such breach is real, immediate, and substantial. If another data breach at Aven occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

127. The hardship to Plaintiff and Class Members, if an injunction does not issue, exceeds the hardship to Aven if an injunction is issued. Among other things, if another massive data breach occurs at Aven, Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Aven of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Aven has a pre-existing legal obligation to employ such measures.

128. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Aven, thus eliminating the additional injuries that would result to Plaintiff and Class Members and all other consumers whose confidential information would be further compromised.

129. Plaintiff and the Class seek actual damages, attorney's fees, costs, and any other just and proper relief available under the laws.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, respectfully request the Court to enter a judgment on their behalf and on behalf of the Class as follows:

a) Certification of the action as a Class Action Pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;

b) That acts alleged herein be adjudged and decreed to constitute negligence, breach of contract, unjust enrichment, and breach of fiduciary duty.

c) A judgment against Defendant for the damages sustained by Plaintiff and the Class defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

d) An order providing injunctive and other equitable relief as necessary to protect the interests of the Class, including, but not limited to:

(1) Ordering that Defendant engages additional third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's

systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

(2) Ordering that Defendant engages additional third-party security auditors and internal personnel to run automated security monitoring;

(3) Ordering that Defendant audits, tests, and trains its security personnel regarding any new or modified procedures;

(4) Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

(5) Ordering Defendant to purge, delete, and destroy in a reasonably secure manner consumer data not necessary for its provisions of services;

(6) Ordering Defendant to conducts regular database scanning; and

(7) Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

e) By awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

f) The costs of this suit, including reasonable attorney fees; and

g) Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all those similarly situated, hereby request a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: January 18, 2024

/s/ Blake G. Abbott
Paul J. Doolittle (Fed ID #6012)
Blake G. Abbott (Fed ID #13354)
POULIN | WILLEY | ANASTOPOULO, LLC
32 Ann Street Charleston, SC 29403
Tel: (803) 222-2222
Email: paul.doolittle@poulinwilley.com
blake.abbott@poulinwilley.com

Attorneys for Plaintiff